Amendment to the Claims:

This listing of claims will replace all versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended)   A method of secure communication comprising:

establishing a secure tunnel between a server and a peer using an encryption algorithm that establishes an encryption key;

authenticating the peer with the server over the secured tunnel establishing an authentication key;

verifying by the server that the peer possesses the same encryption and authentication keys as the first server;

provisioning a network access credential to the peer using the secured tunnel, responsive to the verifying the peer possesses the same encryption and authentication keys as the server; and

signaling an authorization failure to the peer <u>upon conclusion of the provisioning of the network access credential, prior to the peer authenticating using the provisioned credentials,</u> and denying the peer access to the network by the server until the peer authenticates using the provisioned credentials.[[; and]]

~~authenticating using a second authentication protocol by the peer responsive to the authorization failure, wherein the second authentication is performed using the provisioned network access credential.~~ —

2. (Original)   The method of claim 1 wherein the communication implementation between the at least first and second parties is at least one of a wired implementation and a wireless implementation.

3. (Original)   The method of claim 1 wherein the encryption algorithm is an asymmetric encryption algorithm.

4. (Original) The method of claim 3 wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel.

5. (Original) The method of claim 3 wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange.

6. (Previously presented) The method of claim 1 wherein the step of authenticating the peer is performed using Microsoft MS-CHAP v2.

7. (Original) The method of claim 1 further comprising a step of provisioning a public/private key pair on one of the at least first and second parties, and then to provision that public key on the respective remaining ones of the at least first and second parties.

8. (Original) The method of claim 7 wherein the step of provisioning a public/private key pair comprises providing a server-side certificate in accordance with Public Key Infrastructure (PKI).

9. (Currently Amended) An implementation for enabling secure communication comprising:

an implementation for establishing a secure tunnel between server and peer using an encryption algorithm that establishes an encryption key;

an implementation for authenticating the peer with a server using cryptography with an authentication key;

an implementation for verifying by the server that the peer possesses the same encryption and authentication keys as the first part;

an implementation for providing a network access credential to the peer via the secure tunnel responsive to successfully authenticating the peer and verifying by the server that the peer possesses the same encryption and authentication keys; and

an implementation for signaling an authorization failure to the peer upon conclusion of the provisioning of the network access credentials, prior to the peer authenticating using the

provisioned credentials, and denying the peer access to the network by the server until the peer authenticates using the network access credential. [[and]]

~~an implementation for authenticating using a second authentication protocol, the second authentication protocol is performed using the network access credential.~~

10. (Previously presented)   The implementation of claim 9 wherein the implementation for enabling communication between server and peer is at least one of a wired implementation and a wireless implementation.

11. (Original) The implementation of claim 9 wherein the encryption algorithm is an asymmetric encryption algorithm.

12. (Original) The implementation of claim 11 wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel.

13. (Original) The implementation of claim 11 wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange.

14. (Original) The implementation of claim 9 wherein the implementation for authenticating comprises Microsoft MS-CHAP v2.

15. (Previously presented)   The implementation of claim 9 further comprising an implementation for provisioning a public/private key pair on one of the at least server and peer, and then to provision that public key on the respective remaining ones of the at least server and peer.

16. (Original) The implementation of claim 15 wherein the implementation for provisioning a public/private key pair comprises and implementation for providing a server-side certificate in accordance with Public Key Infrastructure (PKI).

Claims 17 - 25 (Canceled)

26. (Previously presented)   The implementation of claim 9, that further comprises:

an implementation for hashing the server encryption key and the server authentication key to produce a first hash;

an implementation for hashing the peer encryption key and the peer authentication key to produce a second hash; and

an implementation for verifying the first and second hash are the same.

Claim 27 (Canceled)

28.   (Previously presented) The method of claim 1, further comprising invalidating a secure credential for the peer responsive to a failure of one of the group consisting of establishing the secure tunnel, authentication, and verifying peer has the same encryption and authentication keys.